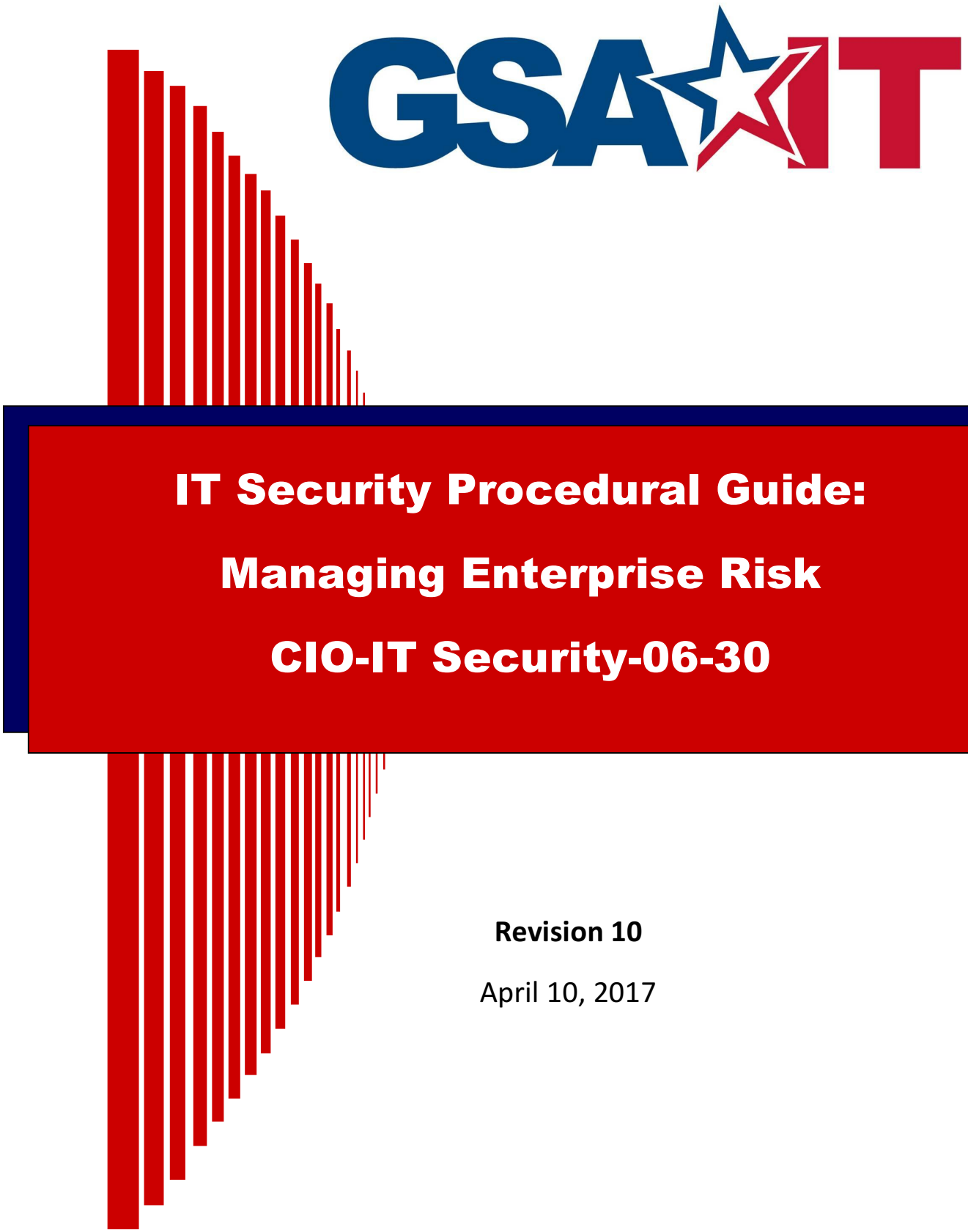

IT Security Procedural Guide:

Managing Enterprise Risk

CIO-IT Security-06-30

Revision 10

April 10, 2017

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 Changes – March 22, 2006				
1	Bo Berlas	Included the OWASP Web Application Penetration Checklist and the OWASP Testing Project documents as embedded objects into Appendix C – GSA Risk Assessment Security Requirements.	To provide a usable checklist for testing the OWASP Top Ten Vulnerabilities.	14
Revision 2 Changes – February 13, 2007				
1	Bo Berlas	Various updates to reflect changes in A&A process	FINAL publishing of NIST 800-53 on 12/2006	4-10
2	Bo Berlas	Updated Appendix A: Risk Assessment Report Format	RA and SA are now combined into a single RA/SA report.	11
3	Bo Berlas	Updated Appendix B: GSA Security Assessment Test Procedures	Updated Assessment test procedures based on FINAL publishing of NIST 800-53 on 12/2006	15
4	Bo Berlas	Updated Appendix C: Plan of Action and Milestone (POA&M) Template	Attached new POA&M template for FY 2007.	16
5	Bo Berlas	Updated Appendix D: Risk Assessment / Security Assessment Plan Template	Updated assessment plan template to reflect combining of RA and SA reports.	17
Revision 3 Changes – March 20, 2007				
1	Bo Berlas	Changed reference to OWASP Top Ten from 2007 Release Candidate 1 back to the 2004 Update.	OWASP Top Ten, 2007 RC1 has not been finalized. GSA will adopt the OWASP Top Ten, 2007 Update upon final publication.	6
2	Bo Berlas	New database scanning requirement.	App Detective or similar tool should be used to test database security configurations.	7
Revision 4 Changes – October 16, 2007				
1	Bo Berlas	Updated policy reference.	GSA IT Security Policy was updated June 2007.	6
2	Bo Berlas	Changed reference to OWASP Top Ten from the 2004 Update to the current 2007 Update.	The 2007 Top Ten lists current web application vulnerabilities.	7

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
3	Bo Berlas	Replaced the FY 2007 POA&M Reporting Template with the FY 2008 template.	New OMB Quarterly POA&M Reporting Requirements	17
Revision 5 Changes – July 15, 2010				
1	Bo Berlas	Update the A&A process to be consistent with NIST 300-37 and the Risk Management Framework	Updates required to ensure agency compliance.	Various
2	Bo Berlas	Inserted Roles and Responsibilities relating to A&A from the GSA IT Security Policy	Identify A&A Roles and Responsibilities	3
3	Bo Berlas	New implementation guidance for NIST 800-53 controls.	To facilitate implementation of required controls	25
4	Bo Berlas	New NIST 800-53 assessment test cases	Required to facilitate assessment of NIST 800-53 controls	Appendix C
5	Bo Berlas	New OCISO A&A Review SOP	Documents the process for submission of A&A packages to the OCISO and the detailed procedural steps performed by the OCISO to verify A&A compliance.	Appendix E
6	Bo Berlas	New guidance for A&A of Minor Systems	To facilitate assessment of minor systems.	22
Revision 6 Changes – December 16, 2010				
1	Bo Berlas	Updated references for Certification, Accreditation, and Certification and Accreditation (C&A) to Assessment, Authorization, and Assessment and Authorization (A&A), respectively.	To be consistent with the current terminology in NIST 800-37.	Throughout
2	Bo Berlas	Inserted guidance for forming sections 1-10 of the SSP for cloud computing system SSPs.	To address cloud specific security challenges.	12
Revision 7 Changes – May 31, 2011				
1	Bo Berlas	Updated references to A&A to security authorization process and authorization package or A&A package to security authorization package.	To be consistent with the current terminology in NIST 800-37.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
2	Bo Berlas	Inserted guidance for review of minimal impact SaaS solutions.	To document required review activities for such systems.	25
3	Bo Berlas	Updated Appendix E to include a revised OCISO Security Authorization Package Review SOP.	To reflect current version of the SOP.	48
Revision 8 Changes – November 25, 2015				
1	Lewis/ Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements	Updated to reflect and implement the most current NIST 800-53-Rev4 and GSA requirements	Various
Revision 9 Changes – May 19, 2016				
1	Wilson/ Klemens	Restructuring of the document, modifications to specific process descriptions.	Updated to reflect current acceptance of risk process and rename Minor Application process to Subsystem process and revise its description. Restructuring and editing throughout.	Various
Revision 10 Changes – April 10, 2017				
1	Desai/ Klemens	Clarifying system definitions and penetration testing requirements.	Included definitions of Federal and Contractor systems. Clarified when systems are required to have penetration tests as part of their assessment.	Sections 1.2, 4.1.7
2	Klemens	Update and edit document.	Updating of hyperlinks, editing of document, updates to align with other GSA documents.	Throughout

Approval

IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30, Revision 10 is hereby approved for distribution.

X

Kurt Garbars
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

The General Services Administration (GSA) agency-wide Security Assessment and Authorization (A&A) Process is based on the National Institute of Standards and Technology (NIST) Risk Management Framework and the security authorization process as described in the latest NIST Special Publication (SP) 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*".

This guide describes key activities in managing enterprise-level risk through a system life cycle perspective including system security authorization and continuous monitoring. It is designed to assist agency and contractor personnel with security responsibilities in implementing the process.

1.1 Purpose

This procedural guide defines the GSA risk management process, specifically the security authorization processes GSA has implemented for information systems to obtain a full authorization to operate (ATO). The guide describes the key activities in managing enterprise-level risk as described in NIST SP 800-37.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal Employees, contractors and associates of GSA who oversee/protect GSA information systems and data. The guide provides GSA associates and contractors as identified in the GSA Order CIO 2100.1, Information Technology (IT) Security Policy, and other IT personnel involved in performing A&A activities, the specific processes to follow for properly accomplishing A&A activities for the systems under their purview. The following definitions are provided for classifying systems within scope of this guide.

- **Contractor System.** An information system processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a Contractor in non-GSA facilities.
- **Agency System (i.e., Federal System).** An information system processing or containing GSA or Federal data where the infrastructure and applications are NOT wholly operated, administered, managed, and maintained by a Contractor in non-GSA facilities.

1.3 Policy

As detailed within CIO 2100.1, Authorizing Officials (AO) must ensure risk assessments are performed as part of A&A activities before a system is placed into production, when significant changes are made to the system and at least every three (3) years unless it is covered by GSA's Continuous Monitoring Program.

1.4 Assessment and Authorization Roles and Responsibilities

There are many roles associated with the security authorization process. System Owners for each information system are responsible for ensuring their respective Service/Staff Office (S/SO) systems have been through the GSA security authorization process, have received an

ATO from the AO, and received concurrence from the GSA Office of the Chief Information Security Officer (OCISO). The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in CIO 2100.1. The following sections provide a high level description of the responsibility for the primary roles with management and operational A&A responsibilities.

1.4.1 GSA Administrator

The GSA Administrator is responsible for ensuring an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of GSA.

1.4.2 GSA Chief Information Officer (CIO)

The GSA Chief Information Officer (CIO) has overall responsibility for the GSA IT Security Program. The CIO is responsible for providing guidance, assistance, and management processes to GSA staff and organizations to enable them to perform their responsibilities with regard to GSA's IT Security Program.

1.4.3 Chief Information Security Officer (CISO)

Public Law 113-283, "*Federal Information Security Modernization Act of 2014*" (FISMA), establishes the designation of a senior agency information security officer responsible for complying with Federal security requirements. GSA has assigned this role to the Chief Information Security Officer (CISO). The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA.

1.4.4 GSA Senior Agency Official for Privacy (SAOP)

The SAOP is responsible for ensuring GSA's compliance with privacy laws, regulations and GSA policy, and the controls in Appendix J: Privacy Control Catalog of NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*". Within GSA, the CIO has designated the Deputy CIO as the SAOP.

1.4.5 Heads of Services and Staff Offices (HSSOs)

HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.4.6 Office of CISO Division Directors

OCISO Directors are the intermediary to the AO for ensuring IT security is properly implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility.

1.4.7 Authorizing Officials (AOs)

AOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority (e.g., the role of Authorizing Official in writing) to appropriately qualified individuals within their organizations.

1.4.8 Information Systems Security Managers (ISSM)

ISSMs report to the ISSO Support Division (IST) Director in the OCISO. There is at least one ISSM per AO. The ISSM is the focal point for all IT system security matters for the systems under their authority. ISSMs are appointed, in writing, by the Director of IST in the OCISO with concurrence by the CISO. An individual appointed as an ISSM for a system cannot also be assigned as the ISSO for the same system.

1.4.9 Information Systems Security Officers (ISSO)

ISSOs are the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO for a system cannot also be the ISSM for the same system. An ISSO is appointed, in writing, by the Director of IST in OCISO with concurrence by the CISO. An ISSO must be knowledgeable of the information and processes supported by the system.

1.4.10 System Owners (i.e., System Program Managers/Project Managers)

System Owners are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk rests with the System Owners. System Owners must ensure their systems and the data each system processes have the necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.

1.4.11 Data Owners (i.e., Functional Business Line Managers)

Data Owners are responsible for determining the security categorization level of systems based upon Federal Information Processing Standards (FIPS) Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems*", and ensuring System Owners are aware of the sensitivity of data to be handled. They must coordinate with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.

1.4.12 Contracting Officers (COs)/Contracting Officer's Representatives (CORs)

COs/CORs are responsible for coordinating and collaborating with the CISO or other appropriate officials to ensure all agency contracts and procurements are compliant with the agency's information security policy. They also must ensure the appropriate security and privacy contracting language is incorporated in each contract and task order.

1.4.13 Custodians

Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. They must coordinate with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

1.4.14 Users of IT Resources

Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures.

1.4.15 System/Network Administrators

System/Network Administrators are responsible for ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.

2 GSA Standard A&A Process

All GSA A&A processes are based upon the NIST SP 800-37 Risk Management Framework (RMF). A depiction of the RMF is provided in Figure 2-1.

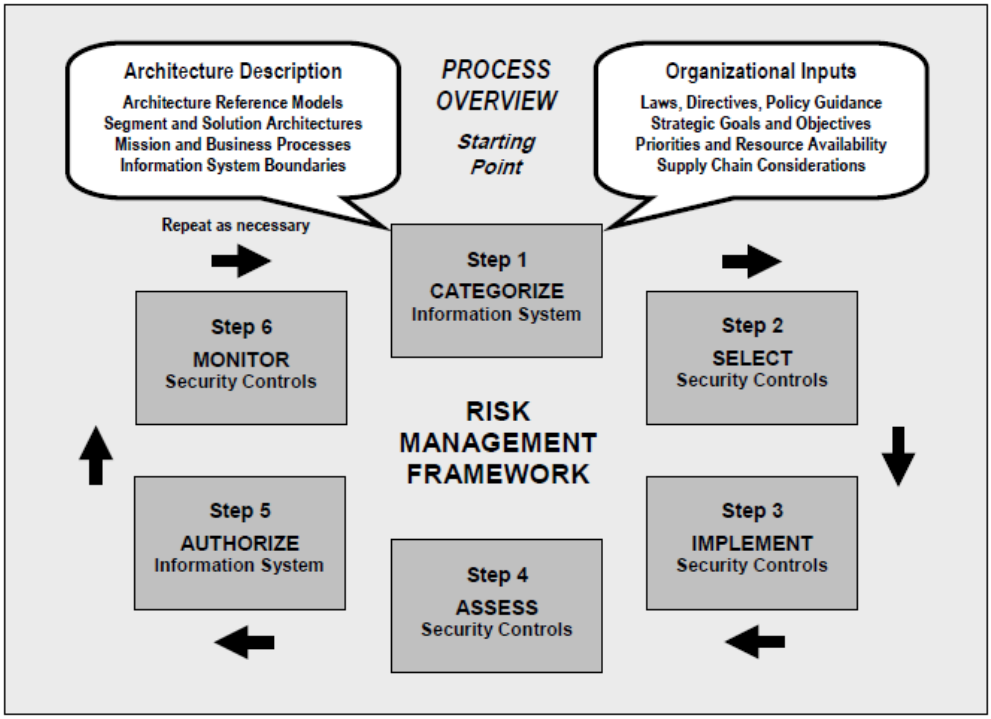

Figure 2-1. Risk Management Framework (from NIST 800-37)

The RMF Steps 1-6 associated with the GSA Standard A&A Process are detailed in the following sections. Additional A&A processes GSA has developed or uses are identified in Section 3 which have been adapted or modified from the standard RMF processes. Documents required as part

of a GSA A&A process are listed in Appendix B along with hyperlinks (where available) to document templates.

2.1 RMF Step 1 – Categorize Information System

The first step in GSA's standard A&A process is to determine the FIPS 199 security categorization level of the information system. This level (Low-, Moderate-, or High-impact) will affect the remaining steps in the process. The following tasks detail the actions in RMF Step 1.

TASK 1-1: Security Categorization - Categorize the information system using the FIPS 199 Security Categorization Template and document the results of the security categorization in the system security plan (SSP). The System Owner carries out the security categorization process in cooperation and collaboration with appropriate organizational officials with information security/risk management responsibilities including but not limited to the Data Owner, AO, ISSM, and ISSO. The process for determining the appropriate impact level is outlined in FIPS 199 and its companion guides, NIST SP 800-60 Volume I, Revision 1, "*Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*" and NIST SP 800-60 Volume II, Revision 1, "*Volume II, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*". Please refer to these documents to categorize the information system. The resulting categorization determines the appropriate security control baseline (Low-, Moderate-, or High-impact) for the information system as outlined within NIST SP 800-53, Revision 4. The baseline is refined in the GSA Control Tailoring Workbook (CTW) to meet GSA's specific needs regarding assignment parameters and applicability of controls.

NOTE: Since forms, templates, and guides are updated frequently, always visit the IT Security Forms and IT Security Procedural Guides pages to ensure the most current version of templates and guides are used.

TASK 1-2: Information System Description - Describe the information system (including system boundary) and document the description in an SSP based on NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*". The SSP provides an overview of the security requirements for the information system, describes the security controls in place or planned for meeting those requirements, and formalizes the plans and expectations regarding the overall functionality of the information system. Descriptive information about the information system is documented in sections 1-12 of the security plan. The level of detail provided in the security plan should be commensurate with the security categorization of the information system. The following sections should be sufficiently detailed:

- Section 2 of the SSP describes the FIPS 199 security categorization of the system. The FIPS 199/NIST SP 800-60 analysis must be supported by a completed FIPS 199 Security Categorization Template.
- Section 9 of the SSP describes the function or purpose of the system and its information processes.
- Section 10 of the SSP contains tables outlining the technical system including an inventory of all assets in the authorization boundary. The tables within this section must be completed and depict a complete inventory of hardware, software and operating

system components. Any subsystems included as a part of the system must be separately identified in Appendix C to the SSP, this appendix will be included as an attachment to the system's ATO Letter.

- Section 11 of the SSP must list all interconnections including the system name, organization, system type; indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 security category, ATO status, and the name of the AO. Per GSA IT Security Policy 2100.1, "Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control IAW NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc."

Contact the OCISO at ispcompliance@gsa.gov with questions or requests for further clarification.

TASK 1-3: Information System Registration - Register the information system with the appropriate organizational program/management offices and security personnel. Inform the OCISO, the System/Application ISSM, and, if different, the ISSM of the larger system on which the system will reside and from which it will inherit security controls. In addition, each IT system is also an IT investment, which needs to be associated with a Unique Investment Identifier.

2.2 RMF Step 2 – Select Security Controls

Based on the FIPS 199 impact level (Low-, Moderate-, or High-impact) determined in Step 1, the appropriate controls will be selected from GSA's CTW which also provides the assignment parameters for the applicable NIST SP 800-53 controls. In RMF Step 2, controls will be identified as system-specific, hybrid, or common; controls will be tailored and supplemented (as necessary) with additional controls and/or control enhancements to address unique organizational or system specific risks; a monitoring strategy will be developed; and the AO's, or designated representative's, approval of the SSP obtained.

The following tasks detail the actions in RMF Step 2.

TASK 2-1: Common Control Identification – Leverage GSA's Information Security Program Plan to identify the GSA common controls and document them in the SSP initiated in RMF Step 1. Common controls are security controls that are inherited. Common control sources may include the OCISO, GSA enterprise systems, S/SO systems, and other sources. System Owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers.

Common control providers are responsible for:

- documenting common controls in a security plan (or equivalent document prescribed by the organization);
- ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization;
- documenting assessment findings in a security assessment report;
- producing a plan of action and milestones for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls);
- receiving authorization for the common controls from the AO; and
- monitoring common control effectiveness on an ongoing basis.

The Common Control Provider's SSP, Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) for common controls (or a summary of such information) should be made available to System Owners (whose systems are inheriting the controls) after the information is reviewed and approved by the AO responsible and accountable for the controls.

A Control Summary Table pertaining to the FIPS 199 impact level associated with the system must be completed. The table identifies controls types (common vs. hybrid controls vs. system specific controls) with implementation status (Fully Implemented, Partially Implemented, Planned, etc.) across required controls. The table should be customized to the GSA S/SO or contractor's environment to account for common controls and subsystems (as necessary). Control Summary Table templates are available for use on the IT Security Forms page (search for "summary" on the web page to ensure the latest summary table is used).

The completed Control Summary table will be included in the appendices section of the SSP. It will be updated in subsequent steps of the RMF process, including after security control implementation and following security assessment to document the results of the review.

TASK 2-2: Security Control Selection - Select the security controls for the information system and document the controls in the SSP. The security controls are selected based on the FIPS 199 security categorization determined in RMF Step 1, Task 1-1, forming the minimum security control baseline for the information system. Once the security controls baseline is determined, it must be tailored by applying scoping, parameterization, compensating control, and GSA guidance. The tailored baselines, as necessary, can be supplemented with additional controls and/or control enhancements to address unique organizational and/or system specific needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

All systems must complete a GSA CTW. The CTW identifies the GSA organizational defined settings for NIST SP 800-53 controls. The selected security controls including any controls or enhancements selected above the baseline for the information system will be documented in both the control tailoring workbook and the SSP. A completed GSA CTW must be included as an

appendix of the system's SSP. Define the settings deferred to S/SO or contractor recommendation to be reviewed and accepted by the GSA AO.

TASK 2-3: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation. The developed strategy may follow the RMF Step 6 - Security Control Monitoring process outlined within Section 2.6.1 of this guide, or the process in IT Security Procedural Guide CIO-IT 12-66, "*Information Security Continuous Monitoring Strategy*" for systems in GSA's Continuous Monitoring Program. The Continuous Monitoring Plan Template described in CIO-IT 12-66 may be used by any System Owner to help form an initial strategy.

TASK 2-4: Security Plan Approval - Review and approve the security plan. The System Owner shall submit the SSP with the following appendices to the ISSO, ISSM, and the AO:

- Required policies and procedures (as requested by GSA)
- Contingency Plan with a Business Impact Assessment (BIA)
- PIA
- Rules of Behavior (as applicable)
- Interconnection Agreements (as applicable)
- GSA CTW
- Control Summary Table

The OCISO will review SSP package to determine if it is complete, consistent, and addresses the security requirements for the information system. Based on the results of the review, the SSP may require further updating or may be approved. The AO or designated AO representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step 3 of the RMF to begin.

The Security Engineering Division (ISE) in the OCISO must review and approve the Security Architecture before the system's security controls are implemented. The OCISO Director of IST must accept the SSP before security control implementation activities can begin. Security Plans will be submitted by the System Owner/Program Manager through the ISSO and ISSM to the Director of IST for review.

2.3 RMF Step 3 – Implement Security Controls

Following the approval received in RMF Step 2, implement the security controls specified in the SSP.

The following tasks detail the actions in RMF Step 3.

TASK 3-1: Security Control Implementation - Security control implementation should be consistent with the GSA enterprise architecture and information security architecture. IT

systems shall be configured and hardened using GSA IT security hardening guidelines (i.e., security benchmarks), NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the AO. Implemented security benchmarks must be integrated with Security Content Automation Protocol (SCAP) content.

To the greatest extent possible, systems are encouraged to conduct initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. Such testing conducted in parallel with the development and implementation of the system facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions.

TASK 3-2: Security Control Documentation - Describe the security control implementation in the SSP, providing a functional description of how the control is satisfied. The security control implementation descriptions should include planned inputs, expected behavior, and expected outputs (where appropriate) that are typical for technical controls. The SSP should also address platform dependencies and include any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment in RMF Step 4.

Security controls are documented in Section 13 of the SSP. This section must provide a thorough description of how the NIST SP 800-53 security controls for the system are being implemented or planned to be implemented. For each control, descriptions must include:

- the security control title;
- how the security control is being implemented or planned to be implemented;
- any scoping guidance that has been applied and what type of consideration;
- identify the control type (Common, Hybrid, App Specific); and
- identify the implementation status (Implemented, Partially Implemented, Planned, N/A, RBD, etc.), and who is responsible for its implementation.

Note: Systems with multiple components or subsystems must describe control implementations across all components.

2.4 RMF Step 4 – Assess Security Controls

Upon implementation of security controls in RMF Step 3, perform a security control assessment to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Complete the tasks below to determine in place security controls, prepare a SAR, and initiate corrective actions based on the findings and recommendations within it.

The following tasks detail the actions in RMF Step 4.

TASK 4-1: Assessment Preparation - Develop, review, and obtain approval for a Security Assessment Plan (SAP) which will be leveraged to assess the security controls of the information system.

The SAP will provide system background information, the objectives for the security control assessment, the assessment approach, and the assessment test cases to be used in Task 4-2. Review, update, and/or supplement GSA's NIST 800-53 Rev4 Test Cases. Add additional assessment test cases for any supplemented controls and/or control enhancements added during Task 2-2, Security Control Selection, to address unique organizational and/or system specific needs.

The following security assessment requirements must be defined in the SAP and implemented for all information systems per its FIPS 199 impact level:

- **FIPS 199 Moderate** and **High** impact systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.
- **All FIPS 199 impact level** information systems must conduct authenticated vulnerability scanning of their servers' operating systems as part of security assessment activities. Configuration/compliance scans shall be to GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, configuration scanning must be to GSA benchmarks. Any scanning tool configured to support the benchmarks or guidelines identified may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool.
- **All FIPS 199 impact level** information systems with web servers must conduct an authenticated vulnerability scan for the most current Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities. Any scanning tool configured to support the OWASP Top 10 may be used. Contact OCISO for information on the current tools in use or if there is a question about a specific tool. If necessary, manual testing and/or verification using the most current OWASP Testing Guide and/or the GSA IT Security Procedural Guide 07-35, "*Web Application Security CIO-IT Security-07-35*" is also acceptable. See the GSA IT Security Technical Guides and Standards web page for links to the OWASP Top Ten Project, the OWASP Testing Guide and CIO-IT 07-35.
- **All FIPS 199 impact level** information systems with database servers must have their databases assessed as part of their OS vulnerability scanning.
- **All FIPS 199 Low and Moderate** impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the Assessment and Authorization (A&A) package.
- **All FIPS 199 impact level** information systems are encouraged (not required) by GSA OCISO to conduct a code analysis using tools to examine the software for common flaws

and document results in a Code Review Report per NIST SP 800-53 Control SA-11 enhancement (1).

Note: The 06-30 Scanning Parameter Spreadsheet contains a listing of scanning frequency by technology type and A&A process.

The SAP must be reviewed and approved by the System Owner, ISSO, and ISSM to ensure that the plan:

- includes all appropriate security controls;
- is consistent with system/organizational security objectives;
- employs required assessment tools and techniques;
- provides assessment test cases; and
- outlines automation to support the concept of continuous monitoring and near real-time risk management.

The overall purpose of the SAP approval is two-fold: (1) to establish the appropriate expectations for the security control assessment; and (2) to bound the level of effort for the security control assessment.

TASK 4-2: Security Control Assessment - Assess the security controls following the SAP and using the NIST 800-53 Rev4 Test Cases updated in Task 4-1 to determine if the controls implemented in RMF Step 3 are operating as intended and producing the desired outcome with respect to meeting the security requirements for the information system.

TASK 4-3: Security Assessment Report (SAR) - Prepare a SAR documenting the issues, findings, and recommendations of the security control assessment. Document the assessment findings with recommendation(s) and risk determinations from the NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. Note that this revision of NIST 800-30 expands the risk rating matrix to five levels; Very Low, Low, Moderate, High, and Very High (equivalent to Critical). Findings in the SAR will be addressed in the following manner:

Findings from Test Cases. Each individual finding must be assessed for risk.

Findings from Vulnerability Scans. Individual findings must be identified; however, findings may be grouped and assessed by level and type of scan. These findings should be assessed in the following groupings and associated with NIST SP 800-53 control SI-2.

1. Very High (Critical)/High OS (includes DB, if applicable) Findings
2. Very High (Critical)/High Web Application Findings
3. Moderate OS (includes DB, if applicable) Findings
4. Moderate Web Application Findings

Findings from Configuration/Compliance Scans. Individual findings must be identified. The findings will be discussed as one group. It will be listed at the Moderate level and associated with NIST SP 800-53 control CM-6.

Low risk findings do not have to be assessed within the SAR; however those findings need to be included in the scan results attached to SAR.

Risk must be determined for findings, as described above, and an overall system or application risk determined. The risk determination will be included as part of the authorization package. Refer to NIST SP 800-30, Revision 1 to ensure that all necessary risk assessment areas are completed.

The risk assessment should consist of the following steps:

- Identifying the list of threats and threat sources to the system. The list should include but not be limited to adversarial outsider and insider threats, accidental user threats, structural threats to its components and facilities, environmental threats to the systems facilities and supporting services;
- Aligning threat sources and events with vulnerabilities;
- Assessing each system instance of absent controls and/or vulnerabilities identified during the security assessment. Evaluate the likelihood the threat sources and events will exploit an identified vulnerability;
- Assess the possible impact to the system and GSA if the vulnerability was exploited;
- Make a determination of risk based on the likelihood the threat will exploit the vulnerability, and the resulting impact, and;
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

The SAR must document all findings from the security assessment that are not FULLY SATISFIED; with vulnerabilities, threats, an in place controls discussion, likelihood, impact, risk discussion/rating, and recommendations for correcting deficiencies in security controls. Assessment results for subsystems, if any, should be included as a subsection to Section 6 – Findings Discussion of the hosting system's SAR. If there is more than one subsystem, a separate subsection should be created for each subsystem.

Note: Review and consider ALL risk categories in the process of preparing the final SAR. It is a common mistake to ignore some classes since they are incorrectly believed to be "low risk". However all scanner tools can categorize findings, in much the same way that false positive findings are not real issues, false negative findings or "low/info risk" findings can be real issues, which a human reader will understand are necessarily more important than initially labeled. Moreover low risk items often enhance the risk of other issues or can successfully be combined to generate higher risk. Once identified, they should be rated appropriately in the final SAR.

FIPS 199 Low or Moderate level systems can possess "High" risk findings the same as FIPS 199 High level systems. All high risk findings must be noted in the SAR.

TASK 4-4: Remedial Action - Conduct initial remediation actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate. Findings that are remediated should be appropriately marked in the SAR. In the SAR, include ''Resolved" next to the NIST SP 800-53 Control Heading.

2.5 RMF Step 5 – Authorize Information System

Following assessment of the information system in RMF Step 4, the POA&M is prepared based upon the results of the security assessment and any remedial action to correct findings; the Security Authorization Package is assembled and submitted to the AO for adjudication. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the overall risk to the agency is acceptable.

Note: GSA tracks all POA&Ms on the POA&M Management Site which serves as the primary tool for the management, storage, and dissemination of GSA system and program POA&Ms.

The following tasks detail the actions in RMF Step 5 – Authorize Information System.

TASK 5-1: Plan of Action and Milestones - Prepare the POA&M from the findings and recommendations in the SAR excluding any remediation actions taken.

Note: External GSA systems and internal GSA systems not being scanning under GSA's vulnerability scanning program must list all individual findings in their POA&Ms in order to provide GSA OCISO visibility into their vulnerabilities.

Develop the POA&M as follows:

- Do not include vulnerabilities identified as ''Resolved" in the SAR.
- Do not include vulnerabilities identified as Very Low/Low risk. These vulnerabilities still need to be included in the SAR either in relation to a NIST control or in the scan results appendices/attachments.
- Moderate, High, and Very High/Critical risk vulnerabilities need to be included in the POA&M.
    - Assessment findings from test cases become individual entries in the POA&M.
    - Findings based on scans are grouped based on the type of scan.
        - Vulnerability scan findings will result in one POA&M entry covering all Moderate and High/Very High (Critical) findings on all components. These vulnerabilities will be managed within GSA's automated scanning tool(s).
        - Configuration/Compliance scans may result in a POA&M entry at the Moderate level for all layers scanned as listed in the 06-30 Scanning Parameter Spreadsheet. A POA&M will be created unless 75% of the system's assets within its FISMA boundary are compliant with 75% of the baseline configuration settings where a GSA hardening guide exists.

The POA&M describes how the System Owner intends to address vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities). Details on developing POA&Ms are contained in the POA&M procedural guide and on the POA&M site. A GSA POA&M Template is available for personnel with POA&M responsibilities who cannot access the POA&M Management site by contacting ispcompliance@gsa.gov. For every Open or Outstanding finding in the SAR (as

described above), there must be a related planned action in the POA&M for the associated NIST SP 800-53 control or enhancement.

Update the SSP to reflect the results of the security assessment and any modifications to the security controls in the information system. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor. Following completion of security assessment activities, the SSP should reflect the actual state of the security controls implemented in the system. Update the GSA CTW and applicable Control Summary Table. The updated documents must be included as appendices to the SSP.

TASK 5-2: Security Authorization Package – The ISSO assembles the security authorization package. The security authorization package includes:

- SSP (with all Appendices and Attachments);
- Security Assessment Report (with all Appendices and Attachments);
- POA&M;
- ATO Letter.

Note: The documents outlined for the Security Authorization Package (above) are required for the GSA Standard A&A Process. The documentation required and links to document templates for other A&A processes GSA uses (and the standard process) are listed in Appendix B.

TASK 5-3: Risk Determination - If an adequate level of information is provided to establish a creditable level of risk, the AO will make a risk level determination. For this determination, the AO assesses all of the information provided by the System Owner as documented in the Security Authorization Package regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks.

TASK 5-4: Risk Acceptance – The explicit acceptance of risk is the responsibility of the AO. The AO determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information. The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision.

A&A Package Review & Approval. The process for reviewing A&A packages for the GSA standard A&A process is as follows.

> The ISSO assembles the security authorization package and submits it to the ISSM for review. The ISSM will review the package, requesting the ISSO address any

inconsistencies/issues. Once satisfied with the package, the ISSM will forward it to the OCISO IST Director.

The OCISO will review the package to provide assurance to S/SO AOs that the systems for which they are responsible have followed required Federal and GSA policy and procedures. Upon completion of this review the OCISO recommends concurrence/non-concurrence to the CISO. The CISO considers this recommendation, collaborates with the AO and others, as necessary, and concurs or non-concurs with granting an ATO based on the security authorization package prior to submitting the ATO Letter to the AO. Concurrences are forwarded to the AO, non-concurrences are returned to the OCISO IST Director.

The AO reviews the completed security authorization package. Based on a determination of the documentation and supporting evidence and whether it establishes an acceptable level of risk the AO may:

- Authorize system operation w/out any restrictions or limitations on its operations;
- Authorize system operation with restrictions/limitations on its operations. The POA&M must include detailed corrective actions to correct the deficiencies requiring the restrictions/limitations. The ISSM/ISSO must resubmit an updated authorization package upon completion of required POA&M actions to move to full ATO without any restrictions/limitations; or
- Not authorize the system for operation.

Note: The System Owner/ISSO must update the SSP and POA&M to reflect any conditions set forth in the ATO letter. Copies of the updated security authorization package including the ATO letter must be distributed to the ISSO, ISSM, System Owner, and the OCISO.

Acceptance of Risk (AOR) Letters. AOR letters are intended for rare or unusual circumstances where the System Owner has limited or no control over the remediation of an identified vulnerability. Examples of such circumstances include:

- Embedded software dependencies
- COTS product update time lines
- Compatibility issues between components

AORs are not intended for delayed or ineffective flaw remediation processes (i.e., patching), insufficient out-year System Development Life Cycle planning (for legacy components), or System Owner preferences. AOR requests must include mitigating factors, compensating controls, and any other action(s) taken to reduce the risk to the system and its data, and a justification for why the vulnerability cannot be resolved. AOR letters have a maximum duration of one year. Upon expiration a new AOR letter may be requested, however it must include new details as to why the vulnerabilities must remain unresolved. AOR letters received without such additional detail will not be approved. Based on the criteria above, AOR letters are:

- Not required for Very Low/Low risk vulnerabilities and findings.

- Required for Moderate risk vulnerabilities and findings. Moderate risk AOR letters require AO approval, but not CISO concurrence.
- Required for Critical/Very High/High risk vulnerabilities and findings. Critical/Very High/High risk AOR letters require AO approval and CISO concurrence.

AOR Letter Processing. AOR letters are processed in the following manner:

1. System Owner/Custodian, ISSO, and ISSM determine the need for an AOR letter based on system POA&Ms.
2. ISSO in conjunction with the ISSM prepares the AOR letter, ensuring an AOR number is added to the footer of the letter.
3. Director of IST notifies the CISO if review and discussions with all stakeholders is appropriate.
4. ISSM submits letter and recommendation to:
    a. AO for approval for Moderate risk vulnerabilities
    b. AO for approval and CISO concurrence for Critical/Very High/High vulnerabilities.
5. Approved document becomes part of the permanent A&A file maintained by the ISSO and ISSM. AOR Letters must be submitted to the OCISO Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.
6. The ISSO is responsible for monitoring POA&Ms and AOR letters. After one year:
    a. If POA&Ms listed in the AOR letter are still unresolved, a new AOR letter is required with additional details on why the vulnerabilities/findings are unresolved.
    b. If all POA&Ms have been resolved, then the AOR letter is noted as completed and archived as a historical record of the system's A&A status.

A&A Documentation Repository. Upon obtaining a signed ATO Letter, the ISSO will upload a copy of all A&A documentation into the A&A Document Repository.

2.6 RMF Step 6 – Security Control Monitoring

2.6.1 Security Control Monitoring

TASK 6-1: Information System and Environment Changes – System Owners must determine the security impact of proposed or actual changes to the information system and its operational environment. Per IT Security Procedural Guide 01-05, "*Configuration Management (CM)*", proposed system changes must be evaluated to determine potential security impacts. An impact analysis of each proposed change will be conducted using the following as a guideline:

- Whether the change is viable and improves the performance or the security of the system;
- Whether the change is technically correct, necessary, and feasible within the system constraints;
- Whether system security will be affected by the change;
- Whether associated costs for implementing the change were considered; and
- Whether security components are affected by the change.

As outlined within GSA's Risk Management Strategy, GSA has a rigorous configuration change management process. The strategy document states that IT changes are requested through a Change Approval Board (CAB) process via a standard CAB form that documents the nature of the change, the criticality, impacts on the user community, testing and rollback procedures, stakeholders, and points of contact. System changes are tested and validated prior to implementation into the production environment. Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CAB process.

TASK 6-2: Ongoing Security Control Assessments – System Owners are responsible for assessing a subset of the NIST SP 800-53 security controls employed within and inherited by the information system in accordance with GSA's monitoring strategy. Per CIO-IT 01-05, the implemented CM process calls for continuous system monitoring to ensure that systems are operating as intended and that implemented changes do not adversely impact either the performance or security posture of the systems. Per GSA's Risk Management Strategy, GSA's annual FISMA self-assessments will assess a subset of security controls, common controls that have been identified as weaknesses for GSA systems in past assessments, and other key controls that GSA has identified. Penetration testing and OIG audits may also be performed for a few selected systems as part of an annual assessment.

TASK 6-3: Ongoing Remediation Actions – ISSOs, System Owners, and System, Network, and Database Administrators, will coordinate and perform remediation actions based upon the results of ongoing monitoring activities, assessment of risk, and outstanding items in the system's POA&M. CIO-IT 01-05 outlines the implementation of a CM process designed to lower the potential risk to a network by requiring regular "patching" or repairing of known vulnerabilities. CIO-IT 01-05 addresses the required steps for implementing changes; Identifying Changes, Evaluating Change Requests, Decision Implementation, and Implementing Approved Change Requests. Per GSA's Risk Management Strategy, risk mitigation shall be the appropriate risk response for all critical and high risks vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Very High/Critical and High risk vulnerabilities must be remediated within thirty (30) days; moderate risk vulnerabilities within ninety (90) days; and low/very low risk vulnerabilities will be addressed on a case-by-case basis. Risk mitigation strategies may include business process improvements, applying timely patches, configuring systems securely, performing secure application code development, and implementing architecture and design modifications as necessary. Risk mitigation measures will be employed based on prioritization. Some of the risk prioritization assessment criteria may include the probability of vulnerability exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, cost and business impact of remediation activities and controls.

TASK 6-4: Key Updates – The System Owner and ISSO will update the following items as part of the system and GSA continuing monitoring plans, processes, and program.

- SSP (and all appendices and attachments)
- SAR (and all appendices and attachments)

- POA&M

The updates will be based on regular updates required by GSA processes, such as:

- Vulnerability scans from GSA's scanning program
- Annual FISMA self-assessments
- Changes identified as part of a system's CM Plan
- Changes identified as part of a system's Continuous Monitoring Plan.

As part of the CM process outlined within CIO-IT 01-05, security testing will be conducted following major or significant system changes. If the changes introduce vulnerabilities, actions to mitigate the vulnerabilities must be included in the system's POA&M, per GSA's POA&M management process, for tracking of the resolution. The SSP will be updated to reflect any changes.

TASK 6-5: Security Status Reporting - The System Owner and ISSO will report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis. GSA's vulnerability scanning program, the GSA POA&M management process, and any required reporting programs will be used to provide security status reporting. AOs and other personnel with security related responsibilities will leverage these resources to keep apprised of the risk levels associated with their system(s).

TASK 6-6: Ongoing Risk Determination and Acceptance – The System Owner, AO, and ISSO will review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with GSA's continuous monitoring strategy and the system's continuous monitoring plan to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation (where applicable) remains acceptable. Data reported via GSA's vulnerability scanning program, the GSA POA&M management process, annual assessments, and other assessment processes (e.g., Penetration Testing, audits, FISMA metrics) will be used by the AO to determine the acceptance of risks and the need to perform reauthorization.

TASK 6-7: Information System Removal and Disposal – System Owners and ISSOs will establish a disposal plan in accordance with NIST SP 800-64, Revision 2, "Security Considerations in the Information System Development Life Cycle", CIO Order 2140.4, "*Information Technology (IT) Solutions Life Cycle (SLC) Policy*", and the GSA Solutions Life Cycle Handbook. In support of this plan, system owners will document the transfer and/or disposal of GSA IT Systems under the provisions outlined within CIO 2100.1, Chapter 3, Section 2.d and IT Security Procedural Guide 06-32, "*Media Protection*".

2.6.2 Information Security Continuous Monitoring Strategy

Inventoried GSA systems that have attained an ATO may request entrance into GSA's Information Security Continuous Monitoring (ISCM) Program. Systems that meet the qualifying requirements of this program no longer follow the three (3) year security authorization process

for GSA information systems. New systems must continue to follow one of the GSA A&A processes to obtain a full three year ATO, including re-authorization every three years, when the system undergoes a significant change or when there is a major security breach impacting the security posture of the system. Specific requirements for admittance into the ISCM Program are detailed in CIO-IT 12-66.

2.6.3 Security Authorization Process Guidance for Significant Changes

Significant changes as defined in NIST SP 800-37, Appendix F, Section F.6, require reauthorization following the security authorization process requirements in this guide. Contact the OCISO at ispcompliance@gsa.gov to determine the scope of reauthorization activities.

2.6.4 Security Authorization Process Guidance for Expiring Authorizations

ISSOs with assistance from the ISP Division can track the expiration dates of ATOs. Renewal of ATOs are initiated by the Authorizing Officials, ISSMs and ISSOs. Per GSA CIO 2100.1 e. (5), *"Information systems with expiring Authorizations to Operate (ATO) may request a one-time extension of the current authorization for a period not to exceed one year from the date of ATO expiration if during this time the system will be decommissioned or to allow development of near real-time continuous monitoring capabilities to support ongoing authorization. ATO extensions must be supported by current vulnerability assessment results (operating system (including database) and web (as applicable)) and POA&M identifying weaknesses from all sources. AOs must obtain approval from the CISO for the continuous monitoring plans of systems authorizations that have been extended. Plans must be approved within 6 months of the extension."*

Questions concerning the security authorization process, significant changes, or expiring ATOs can be directed to ispcompliance@gsa.gov.

3 Security Authorization Process

In addition to the GSA Standard A&A Process, GSA has implemented several other A&A processes for the purpose of ensuring risks to GSA IT resources are reduced to the extent possible based on budget constraints, business requirements and other resource issues. These processes and the criteria required for each are outlined below. The specific details describing each of the processes may be found in the document listed in "Document Reference" in Section 3.2 for each assessment type. Regardless of which A&A process is followed, before assessment activities for information systems begin, the following requirements must be met:

(1) The SSP is approved.

(2) The information system's architecture is approved by the OCISO Security Engineering Division (ISE).

(3) The SAP is approved.

3.1 Identifying the Appropriate A&A Process/Program

Table 3-1 identifies the criteria to qualify for each A&A process.

Table 3-1. A&A Process Requirements

A&A Process/Program	Qualifying Criteria
Standard GSA Process	• All new and existing GSA information systems that do not fall under one of the other A&A processes
Lightweight Security Authorization Process	• New GSA information systems pursuing an agile development methodology • Reside on infrastructures that have a GSA ATO concurred to by the CISO or a Federal Risk and Authorization Management Program (FedRAMP) ATO • Must be FIPS 199 Low or Moderate
GSA Salesforce Process	• Applicable to applications that integrate into the main Salesforce.com application and are hosted on Salesforce.com's infrastructure • Applications developed for internal and external GSA use published on the Salesforce Platform
Security Reviews for Low Impact Software as a Service Solutions Process	• Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA • Duration is limited and/or one time use • Data already exists in the public domain or data is non-sensitive and is considered FIPS 199 Low impact • GSA would not be harmed regardless of the consequence of an attack or compromise • Dollar cost for such deployments do not exceed $100,000 annually
GSA Agency FedRAMP Process	• A Cloud Service Provider (CSP) requesting GSA Agency sponsorship into FedRAMP • GSA accepts sponsoring the CSP • GSA determines CSP's security authorization package will be considered FedRAMP compliant
Security Reviews for Moderate Impact Software as a Service Solutions Process	• Dollar cost for such deployments do not exceed $100,000 annually • Must be FIPS 199 Moderate • Vendor has had an external assessment done such as a SOC 2/SSAE 16 or FedRAMP approval within the past year • If not FedRAMP approved, must be enrolled in the FedRAMP certification process
GSA Subsystem Process	• Classified as a subsystem (and not a Salesforce application) • Majority of it security controls provided by the GSS/MA in which it operates • FIPS 199 Low or Moderate • FIPS 199 level can be below the level of the host GSS or MA

A&A Process/Program	Qualifying Criteria
GSA Continuous Monitoring Program	• Must be an inventoried GSA system with an ATO • Underlying hosting system must be in GSA's continuous monitoring program (contact OCISO if this criteria is a roadblock) • Has implemented automated continuous monitoring capabilities • SSP and POA&M up to date • Develop a Continuous Monitoring Plan

3.2 A&A Process Descriptions

Additional details about the GSA A&A processes listed in Table 3-1 are provided in the following sections:

3.2.1 GSA Standard A&A Process

- **Document Reference**: Throughout this guide, process steps are described in Section 2.
- **Result**: Full 3 Year ATO
- **Summary of Process**: All new and existing GSA information systems must undergo a security assessment and authorization at least every three (3) years or whenever there is a significant change to the system's security posture. The result is an ATO for a period not to exceed three (3) years. Specific requirements are detailed throughout this guide.
- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.2 Lightweight Security Authorization Process

- **Document Reference:** IT Security Procedural Guide: Lightweight Security Authorization Process" (GSA CIO-IT Security-14-68)
- **Result:** Limited ATO (LATO) - 90 day (Sprint or Standard)/1 Year (Moderate), Full 3 Year ATO (Low)
- **Summary of Process:** New GSA information systems pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO. The process allows for an initial 90-day LATO for Low and Moderate pilot systems to support integration, testing, and limited production capabilities (as defined by the GSA CISO). Systems, including those with a 90-day LATO, can be granted a one year LATO for FIPS 199 Moderate impact systems and a full three-year ATO for FIPS 199 Low impact information systems after completing the complete RMF process detailed in CIO-IT 14-68.

  A 90-day LATO can be issued based on the results of a limited assessment (e.g., vulnerability scans, penetration tests) described in CIO-IT 14-68. The following documents are required to issue a 90-day LATO:

  - Assessment Test Report (i.e., Enhanced Scanning and Assessment, Penetration)
  - POA&M
  - ATO Letter

A one year LATO (for FIPS 199 Moderate) or a three-year full ATO (for FIPS 199 Low) can be issued based on competing RMF Steps 1-5 as described in CIO-IT 14-68. The following documents are required:

- SSP
- SAR, including
  - Assessment Test Cases
  - OS (including DB), Web App scan data (as appropriate)
  - Penetration Test Report
- POA&M
- Customer Responsibility Matrix (CRM)
- ATO Letter

- **A&A Package Review & Approval Process**: Follows the process described in Section 2.5.

3.2.3 GSA Salesforce Platform Process

- **Document Reference:** IT Security Procedural Guide: GSA's Security Implementation of the Salesforce Platform (GSA CIO IT Security 11-62)

- **Result:** Salesforce Application ATO

- **Summary of Process**: Specific to applications developed for internal and external GSA use published on the Salesforce Platform. The first step is to determine the type of application. If the application is a major application, then a full Assessment and Authorization is required. If the application is a subsystem, there are key activities that should be completed. Applications are assessed and authorized in accordance with this guide, Salesforce Organization Baseline Security Configuration Settings, and specific requirements detailed in CIO-IT 11-62.

- **A&A Package Review & Approval Process**: After the ISSM accepts/approves the A&A package it is forwarded to the CISO for signature (i.e., no OCISO Director review).

3.2.4 Security Reviews for Low Impact Software as a Service Process

- **Document Reference:** IT Security Procedural Guide 16-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions"* describes the process and requirements for authorizing the operation of Low Impact SaaS solutions within GSA.

- **Result:** 1 year ATO or term of license, whichever is shorter

- **Summary of Process:** Private sector cloud computing Software as a Service (SaaS) solutions that are implemented within GSA for (1) limited duration and/or one time use; (2) involve data already in the public domain or data that is non-sensitive and could be considered FIPS 199 low impact, (3) GSA would not be harmed regardless of the consequence of an attack or compromise; and, (4) if the dollar cost for such deployments do not exceed $100,000 annually. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the

data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk. The ATO shall only be valid for the period of the time the application license is valid or one (1) year, whichever is shorter.

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5.

3.2.5 FedRAMP Process

Document Reference: Guide to Understanding Federal Risk and Authorization Management Program (FedRAMP), additional details available in the FedRAMP Security Assessment Framework and FedRAMP Standard Operating Procedures & Checklists

- **Result:** FedRAMP ATO (Agency)
- **Summary of Process:** A Cloud Service Provider (CSP) may elect to request an Agency FedRAMP ATO from GSA. It is at the discretion of GSA to accept or deny the CSP's request for sponsorship. CSPs which GSA agrees to sponsor for a FedRAMP authorization are required to follow the FedRAMP PMO authorization process requirements. GSA has defined assignments for NIST SP 800-53 control parameters within the FedRAMP Low and Moderate baselines as its organizationally defined parameters. The parameters are contained in Appendix C. Additional information about FedRAMP is available in the reference documents and at https://www.fedramp.gov/. The CSP must provide a security authorization package to GSA. If GSA determines the package to be FedRAMP compliant, the CSP in cooperation with GSA will pursue a FedRAMP ATO.

  System Owners/AOs with questions about leveraging the FedRAMP security authorization process (to attain a Government wide authorization) should contact the OCISO at ispcompliance@gsa.gov.

- **A&A Package Review & Approval Process**: Follows the FedRAMP process.

3.2.6 GSA Moderate Software as a Service (SaaS) Solutions Process

- **Document Reference:** An IT Security Procedural Guide for Security Reviews for Moderate Impact Software as a Service (SaaS) Solutions has been in development and will be available on the IT Security Procedural Guides webpage when published.
- **Result:** 1 Year ATO
- **Summary of Process:** Specific to applications: (1) the dollar cost of such deployment does not exceed $100,000 annually, (2) determined to be FIPS-199 Moderate impact system, (3) data center security is qualified by a current Standards for Attestation Engagements (SSAE) 16/ Service Organization Control (SOC) 2, or Federal Risk and Authorization Management Program (FedRAMP) approval, must be enrolled in the FedRAMP certification process. AOs must consider Federal and agency information

security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk. The ATO shall only be valid for one (1) year. Approved Moderate SaaS applications become subsystems of the Enterprise Cloud Services (ECS) system.

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5.

3.2.7 GSA Subsystem Process (previously Minor Application Process)

- **A&A Process Reference:** Described within this section.
- **Result:** ATO aligned with subsystem's hosting/supporting system.
- **Summary of Process:** This process is specific to subsystems (other than Salesforce applications) categorized with a FIPS 199 security impact level of Low or Moderate , dependent upon the resources provided by its underlying hosting/supporting system, with the underlying system providing the majority of the subsystem's security controls. The hosting/supporting system must be shown to provide a foundational level of protection for the subsystem; the subsystem may have a FIPS 199 level equal to or below the level of its hosting/supporting system.

  Subsystems with a FIPS 199 security impact level of Low will adhere to and implement the controls per CIO-IT 14-68.

  Subsystems with a FIPS 199 security impact level of Moderate will document in a subsystem SSP all controls identified as hybrid or system specific by the underlying hosting/supporting system. These controls will be assessed using GSA's NIST 800-53 Test Cases and the results shared with the hosting/supporting system's System Owner/ISSO. All subsystems will be identified in an Appendix of their hosting/supporting system's SSP which will also be attached to the hosting/supporting system's ATO Letter. All subsystems inherit its hosting/supporting system's ATO cycle.

- **A&A Package Review & Approval Process**: Subsystems are included in the A&A Package Review & Approval Process of their hosting/supporting system. No separate ATO is issued for subsystems.

3.2.8 GSA Continuous Monitoring Program

- **A&A Process Reference:** IT Security Procedural Guide: Information Security Continuous Monitoring Strategy CIO-IT Security-12-66
- **Result:** Ongoing Authorization based on continuous monitoring
- **Summary of Process:** The GSA Continuous Monitoring Program replaces the three (3) year security authorization process for GSA information systems that meet its qualifying

requirements with an ongoing authorization process. The GSA Continuous Monitoring baseline controls are assessed in two ways; (1) Controls identified as automated will be verified via both self-attestation and enterprise-level oversight performed by the OCISO using reports and feeds generated using automated tools, (2) Manual controls or process-based controls are vetted via either self-attestation or self-attestation with supporting deliverable. All self-attestations are due annually together with the annual FISMA self-assessment and continuous monitoring plan update. In cases where security controls are determined to be inadequate, the continuous monitoring program facilitates prioritized security response actions based on risk.

- **A&A Package Review & Approval Process**: Follows the same process described in Section 2.5, with the following exception, the Director of ISP replaces the Director of IST.

4 GSA Implementation of CA, PL, and RA Controls

NIST SP 800-53 defines controls related to the security authorization process that GSA is required to implement based on an information system's security categorization. The Security Assessment and Authorization (CA), Planning (PL), and Risk Assessment (RA) control family implementations are addressed in this guide.

Note: The GSA IT ISPP was developed to provide stakeholders with detailed information on the NIST SP 800-53 controls GSA has considered inheritable common and hybrid controls and who the responsible party is for implementing the control. In the following sections when a control implementation is covered in the ISPP the control's subsection will refer to the ISPP for parameter assignments and implementation guidance.

4.1 Security Assessment and Authorization (CA)

4.1.1 CA-1 Security Assessment and Authorization Policy and Procedures

Parameter assignments and implementation guidance for the CA-1 control are provided in the ISPP.

4.1.2 CA-2 Security Assessments

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation [*annually*] to determine the extent to which the controls are implemented

correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Acquisitions/Contracting Officers, Custodians].

Control Enhancements:

(1) The organization employs assessors or assessment teams with [the use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.] to conduct security control assessments

(2) The organization includes as part of security control assessments, [annual], [announced], [penetration testing].

GSA Implementation Guidance:

GSA requires a security control assessment to be performed for all information systems as part of the security authorization/re-authorization process. The security control assessment must include GSA's NIST 800-53 Test Cases. The security control assessment must document the implementation status in sufficient detail in order to assist in determining the overall effectiveness of all controls and enhancements that have been selected and implemented for the system as per FIPS-199 impact level.

GSA's process for performing a security control assessment is fully defined in Section 2.4 of this guide, RMF Step 4 – Assess Security Controls. The results of the security control assessment must be documented in a SAR.

As per CA-2, Enhancement (1), GSA FIPS 199 Moderate and High Impact Systems must be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls.

CA-2, Enhancement (2), requires GSA FIPS High Impact Systems to be assessed annually, via announced penetration tests. Penetration testing provides a more thorough analysis of the implementation effectiveness of security controls associated with an information system.

Additional Contractor System Considerations: *None.*

4.1.3 CA-3 System Interconnections

Control: The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [*at least annually*].

Control Enhancements:

(5) The organization employs [*deny-all, permit-by-exception*] policy for allowing [*all GSA systems*] to connect to external information systems.

GSA Implementation Guidance:

The focus of this control is to ensure that any persistent connection to any other information system outside of the system's authorization boundary has been approved by the AO, identified and documented within the SSP, and monitored on an ongoing basis.

Chapter 3 of GSA CIO 2100.1 outlines the following interconnection requirements:

Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control in accordance with NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems." Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc.

If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system; and

All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the GSA CISO.

The terms "connection" or "interconnection" in this case, means any on-going, persistent or substantial interaction with any information system(s) that is located outside of the authorization boundary. These connections can be physical and/or logical, and include data entering or exiting to/from the authorization boundary. User-controlled connections such as email, ftp, remote access, and web browsing are not considered interconnections and therefore do not apply to this control.

Additional Contractor System Considerations: None.

4.1.4 CA-5 Plan of Action and Milestones

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [*quarterly*] based on the findings from security impact analyses, and continuous monitoring activities.

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems have developed a POA&M in accordance with CIO-IT 09-44 which details the POA&M processes and procedures for meeting the requirements of this control.

A quarterly POA&M report must be submitted to the OCISO in order to monitor agency-wide remediation efforts as required by OMB policy. These updates must be performed for each quarter of the fiscal year using the GSA POA&M Template which is maintained by the system ISSO or ISSM and uploaded to the POA&M Management Site for OCISO review. The POA&M Management Site serves as the primary page for managing and communicating GSA's system and program POA&Ms, and is available internally at GSA, or from the web via VPN. New systems that are currently undergoing security authorization process or that have not been included in the GSA FISMA inventory must use the POA&M Template available on GSA InSite.

Additional Contractor System Considerations:
Contractor systems must submit POA&Ms through their Government ISSO(s) as contractors will not have access to the POA&M Management Site. Government ISSOs supporting these systems must facilitate POA&M updates by sending the current version of the system POA&M together with the quarterly OCISO guidance to the contractor representative(s). Upon receipt of the POA&M from the contractor, Government ISSOs shall review the POA&M to ensure it is updated and includes required vulnerabilities, before posting the POA&M to the GSA POA&M Management Site.

4.1.5 CA-6 Security Authorization

Control: The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [every three (3) years or when a significant change occurs as defined in NIST SP 800-37, Revision 1, Appendix F, Section F.6].

GSA Implementation Guidance:
The focus of this control is to ensure that all information systems which have been authorized to operate before being placed into operational status. All information systems must undergo

authorization/reauthorization every three years or when there is a significant change as defined in NIST SP 800-37, Appendix F, Section F.6, following the security authorization process documented in this guide. Detailed procedures for the security authorization process can be found in Section 2.5 of this guide, RMF Step 5 – Authorize Information System. Additional ATO or authorization types exist in GSA and are described in Section 3.2 of this document.

The explicit acceptance of *risk* is the responsibility of the AO. The AO must consider many factors, balancing security considerations with mission and operational needs. The AO issues an authorization decision for the information system and the common controls inherited by the system after reviewing the security authorization package submitted by the System Owner. The security authorization package provides the AO with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The security authorization package includes:

- SSP (required policies and procedures (as requested by GSA), Rules of Behavior, Interconnection Agreements (as applicable), GSA 800-53 Control Tailoring Workbook, and appropriate Control Implementation Summary Table);
- Security Assessment Report (with required appendices [see Appendix B]);
- POA&M;
- Independent Penetration Test Report, if applicable;
- Code Review Report (Strongly Recommended);
- Contingency Plan;
- Contingency Plan Test Report; and
- ATO Letter.

The AO must determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, assets, and individuals and determine if the risk to the agency is acceptable. Following review of the security authorization package and consultation with key agency officials, the AO must render an authorization decision to:

- Authorize system operation w/out any restrictions or limitations on it operation;
- Authorize system operation w/ restriction or limitation on its operation. The POA&M must include detailed corrective actions to correct deficiencies. Resubmit an updated security authorization package upon completion of required POA&M actions to move to ATO w/out any restrictions; or
- Not authorized for operation.

Questions concerning the security authorization process, significant changes, or CIO 2100.1 can be directed to ispcompliance@gsa.gov.

Additional Contractor System Considerations: *None.*

4.1.6 CA-7 Continuous Monitoring

Parameter assignments and implementation guidance for the CA-7 control are provided in the ISPP.

CIO IT Security 12-66 provides detailed information on the implementation of GSA's Information System Continuous Monitoring Program.

4.1.7 CA-8 Penetration Testing

Control: The organization conducts penetration testing [*during A&A efforts and annually thereafter*] on [*all Internet accessible systems, and all FIPS 199 High impact systems*.]

NOTE: Independence is waived for all annual testing (i.e., testing can be internally performed).

Control Enhancements:

(1) The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

GSA Implementation Guidance:
All Internet accessible systems, and all FIPS 199 High impact systems are required to complete an independent penetration test and provide an Penetration Test Report documenting the results of the exercise as part of the A&A package. Annual penetration tests can be completed internally and do not require an independent assessor.

Additional Contractor System Considerations: *None.*

4.1.8 CA-9 Internal System Connections

Control: The organization:

a. Authorizes internal connections of [*if GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system*] to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

GSA Implementation Guidance:
If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system

4.2 Planning (PL)

4.2.1 PL-1 Security Planning Policy and Procedures

Parameter assignments and implementation guidance for the PL-1 control are provided in the ISPP.

4.2.2 PL-2 System Security Plan

Control: The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*];

c. Reviews the security plan for the information system [*annually*];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

Control Enhancements:

(3) The organization plans and coordinates security-related activities affecting the information system with [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*] before conducting such activities in order to reduce the impact on other organizational entities.

GSA Implementation Guidance:

The focus of this control is to ensure that a SSP has been developed for the information system that documents the security requirements for the information system, and the implementation status of the security controls that have been assigned to the system as per FIPS 199 impact analysis. All GSA information systems must develop a SSP in accordance with this guide and NIST SP 800-18. Detailed guidance is available in sections RMF Step 1 – Categorize Information System and RMF Step 3 – Implement Security Controls of this guide.

The security requirements per FIPS-199 impact level and the security controls which are planned or in-place to meet these requirements, must be documented within the SSP and updated as-needed to reflect any change to the information system environment. Updates made to the SSP must include updates to system applications and hardware, remediation of previously identified weaknesses and any addition of new weaknesses identified through security assessments or continuous monitoring.

Additional Contractor System Considerations: *None.*

4.2.3 PL-4 Rules of Behavior

Parameter assignments and implementation guidance for the PL-4 control are provided in the ISPP.

4.2.4 PL-8 Information Security Architecture

Control: The organization:

a. Develops an information security architecture for the information system that:
    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture [at least annually] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

GSA Implementation Guidance:
Reviews and updates the information security architecture annually to reflect updates in the enterprise architecture; GSA's Security Engineering Framework requires every system seeking authorization to have their architecture approved by ISE before beginning security assessment activities.

4.3 Risk Assessment (RA)

4.3.1 RA-1 Risk Assessment Policy and Procedures

Parameter assignments and implementation guidance for the RA-1 control are provided in the ISPP.

4.3.2 RA-2 Security Categorization

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

GSA Implementation Guidance:
GSA system owners, data owners, ISSOs, and ISSMs are required to follow the processes and procedures described in Section 2.1 of this guide for determining the security categorization of their information and information systems.

Additional Contractor System Considerations: *None*

4.3.3 RA-3 Risk Assessment

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [*Security Assessment Report (SAR*)];
c. Reviews risk assessment results [*every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 1, Appendix F, Section F.6*]; and
d. Disseminates risk assessment results to [*Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), Custodians*]; and
e. Updates the risk assessment [*every three (3) years or with a significant change as defined in NIST SP 800-37 Revision 1, Appendix F, Section F.6*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

GSA Implementation Guidance:
The focus of this control is to verify that an assessment of risk is performed and documented for the information system and that the subsequent security assessment report is communicated to GSA senior management, in order to provide key information regarding the system's current security state and resulting risk to GSA operations, assets, and individuals. The results of the risk assessment provide critical information to assist the GSA AO in determining whether or not to authorize/re-authorize the information system.

GSA requires a risk assessment to be conducted as part of the initial security authorization process, then every three years or whenever a significant change occurs as defined in NIST SP 800-37, Appendix F, Section F.6. GSA's process for performing a risk assessment is fully defined

in Section 2.4 of this guide. The results of this risk assessment must be documented in the SAR template.

Additional Contractor System Considerations: *None*

4.3.4 RA-5 Vulnerability Scanning

Parameter assignments and implementation guidance for the RA-5 control are provided in the ISPP.

5 Summary

Managing enterprise-level risk through a system life cycle perspective is a departure from the traditional view of security authorization as a static, procedural process. The policies and procedures outlined in this guide provide an effective approach to system security authorization that is more dynamic and more capable of managing information system-related security risks across a diverse enterprise.

This guide describes GSA's agency-wide security authorization processes in accordance with NIST RMF and the security authorization process as described in NIST SP 800-37, Revision 1.

All GSA information systems must undergo security control assessment and be authorized to operate according to their specific process, GSA's standard A&A process requires A&A at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37, Revision 1.

GSA contractors and Federal employees should use this guide and the noted references prior to selecting and performing a security authorization process. Where there is a conflict between NIST guidance and GSA guidance, contact OCISO at ispcompliance@gsa.gov.

Appendix A: Consolidated List of Guidance, Policies, Procedures

Federal Guidance:

- NIST Special Publication (SP) 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems"
- NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations"
- FIPS 199, Standard for Security Categorization of Federal Information and Information Systems
- NIST SP 800-60, Volume I, Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-60, Volume II, Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"

GSA Guidance:

- GSA CIO Order 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA CIO-IT Security-06-30, "*Managing Enterprise Risk*"
- GSA CIO-IT Security-14-68, "*Lightweight Security Authorization Process*"
- GSA CIO-IT Security-11-62, "*GSA's Security Implementation of the Salesforce Platform*"
- GSA CIO-IT Security-12-66, "*Information Security Continuous Monitoring Strategy*"
- GSA CIO-IT Security-09-48, "*Security Language for IT Acquisition Efforts*"
- GSA CIO-IT Security-16-75, "*Security Review for Low Impact Software as a Service (SaaS) Solutions*"
- GSA CIO-IT Security-11-51, "*Conducting Penetration Test Exercises*"
- GSA CIO-IT Security-09-44, "*Plan of Action and Milestones*"
- GSA Information Security Program Plan

Appendix B: A&A Process Package Document Lists/Links

This Appendix contains a listing of the A&A Package documentation requirements for each of the A&A processes described in this guide, where possible hyperlinks to applicable documents and templates have been provided.

Standard A&A Process
Documents
System Security Plan (Low, Moderate, High) Appendix A - Acronyms, Terms, and Definitions Appendix B - References Appendix C - Hosted Subsystems (if applicable) Other Appendices, as necessary Attachment 1: Privacy Threshold Analysis / Privacy Impact Assessment Attachment 2: FIPS 199 Security Categorization Attachment 3: e-Authentication Assurance Level Attachment 4: Interconnection Security Agreement Attachment 5: GSA Control Tailoring Workbook Attachment 6: Control Summary Table Control Summary Table Low Control Summary Table Moderate Attachment 7: Contingency Plan Contingency Plan for Low Impact System Contingency Plan for Moderate Impact System Contingency Plan for High Impact System Attachment 8: Contingency Plan Test Report Attachment 9: Incident Response Plan Attachment 10: Incident Response Plan Test Report Attachment 11: Configuration Management Plan Attachment 12: Continuous Monitoring Plan (if applicable) Attachment 13: Rules of Behavior (if applicable) Attachment 14: Code Review Report (if applicable) Other Attachments, as necessary
Security Assessment Report (Results from the Security Assessment Plan) Appendix A - Acronyms, Terms, and Definitions Appendix B - NIST 800-53 Test Cases Appendix C - Operating System Scanning Results Appendix D - Database Application Scanning Results Appendix E - Web Application Scanning Results Other Appendices, as necessary Attachment 1: Penetration Test Report Other Attachments, as necessary
Plan of Action and Milestones (POA&M)
ATO Letter

Lightweight Security Authorization Process
Documents
System Security Plan AWS System Security Plan Template CGI System Security Plan Template
Security Assessment Report AWS Security Assessment Report CGI Security Assessment Report
Select GSA NIST 800-53 Security Assessment Test Cases AWS Security Assessment Test Cases CGI Federal IaaS Cloud Security Assessment Test Cases
Customer Responsibility Matrix AWS Customer Responsibility Matrix CGI Customer Responsibility Matrix
Vulnerability Scan Data
Penetration Test Report
ATO Letter

GSA Salesforce Process
Documents
GSA CIO-IT Security-11-62, "*GSA's Security Implementation of the Salesforce Platform*", contains specific instructions concerning the Salesforce-specific templates identified below (identified by an asterisk) and where a URL is not available.
*Implementation of Subsystems * a. COE Security Process 2016 * b. App Config Example * c. Security Controls Analysis Template * d. Salesforce App Review Process Template
*Salesforce Guide 11-62 Section 4_8 Controls
*Salesforce Security Plan Customer Controls - This document is controlled and is available by contacting the Salesforce ISSM or ISSO.
*Example Salesforce Organization Baseline
*SF Security Settings
*Salesforce Security Impl. Guide - Spring 2016
*A Guide to Sharing Architecture
*SF Security Configuration Options
*User Request Form Salesforce Template
*External Access to GSA Salesforce User
Privacy Threshold Analysis / Privacy Impact Assessment
Code Scan Reviews
Plan of Action and Milestones (POA&M)
ATO Letter

Security Reviews for Low Impact Software as a Service Solutions Process
Documents
Documented results of required review activities, including:
Assign a unique ID to each person. Users must be individually identified (Reference NIST SP 800-53 control IA2 - Identification and Authentication). When possible, Two Factor Authentication (2FA) should be used for user logons.
Document and implement system and security parameters deferred to customers. Do not use the vendor-supplied defaults for system passwords and other security parameters. GSA security policies and best practices should be used to the greatest extent possible.
All transmissions of authentication credentials must be encrypted (e.g., TLS over HTTPS). It is strongly recommended that the entire session be encrypted.
Perform web application scanning (e.g., WebInspect, Acunetix, Burp Suite Pro, etc.) annually. The OCISO can assist with web application scans if vendor(s) do not have an in house web application scanning capability.
Perform operating system (OS) vulnerability scanning (e.g., Nessus, Qualys, nCircle, McAfee Vulnerability Manager, etc.). a. Vendors that are Payment Card Industry Data Security Standard (PCI DSS) compliant or have the McAfee Secure Seal or TrustGuard Quarterly Scanned Seal must provide the results of their latest PCI DSS Compliant, McAfee Secure Seal or TrustGuard quarterly scan. b. Vendors that do not meet the PCI DSS, McAfee, or TrustGuard standards listed, must provide their most recent OS vulnerability scan results.
Verify that the vendor has an acceptable flaw remediation process exists. Vendors must be able to identify and remediate information system flaws in a timely manner (i.e., how often scans are completed and how vulnerabilities are remediated). Reference NIST 800-53 control SI2 – Flaw Remediation.
Vendor shall either provide the results of their Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 16 audit report and/or have one of the following vendor certifications SysTrust, WebTrust (American Institute of Certified Public Accountants (AICPA)-sponsored), ISO/IEC 27001, or PCI DSS Compliance. The SSAE/SOC 2 is not a form of security certification but it does provide independent third party attestation of the provider's general operating environment and supporting processes. Vendors may also provide evidence of PCI security assessments, self-testing, and records from other external audits and assessors to supplement the SSAE/SOC 2 audit report or vendor certifications. Vendors are strongly encouraged to present as much information as possible to allow an adequate understanding of the applications security posture and a determination of risk. Although the minimum requirement is for the SSAE/SOC 2 audit report or one of the vendor certifications; the GSA AO and the CISO will take a holistic view of the application based on all of the documentation presented to determine the overall risk of the application as well as any residual risks that may need to be accepted when considering the application for use. If the documentation presented does not provide an adequate understanding of the systems security posture and/or is deemed insufficient to make a risk determination; additional information will be required.
ATO Letter

GSA Agency FedRAMP Process
Documents
Note: The FedRAMP A&A documentation templates are available on the FedRAMP website under Documents and Templates. Please visit that website to get the current templates.
System Security Plan
Security Assessment Plan
NIST 800-53 Revision 4 Test Cases
Security Assessment Report
(Vendors) Users Guide)
Control Implementation Summary
Plan of Action and Milestones
FIPS 199 Categorization
e-Authentication Level
Rules of Behavior
(Vendors) Configuration Management Plan
(Vendors) Information System Security Policies
IT Contingency Plan
(Vendors) Incident Response Plan
Privacy Threshold Analysis and PIA

Security Reviews for Moderate Impact Software as a Service Solutions Process
Documents
An IT Security Procedural Guide for Security Reviews for Moderate Impact Software as a Service (SaaS) Solutions has been in development and will be available on the IT Security Procedural Guides webpage when published.
Until a guide for Moderate Impact Software as a Service (SaaS) Solutions is published, complete the same documentation as listed for Low Impact Software as a Service (SaaS) Solutions and other documentation as required by the AO or OCISO.

GSA Subsystem A&A Process
Documents
FIPS 199 Low Subsystem
See Lightweight Security Authorization Process Documentation)
FIPS 199 Moderate Subsystem
System Security Plan (Low, Moderate, High) (hybrid and system specific controls)
NIST 800-53 Test Cases (hybrid and system specific controls)
Security Assessment Report (hybrid and system specific controls)

GSA Continuous Monitoring Program
Documents
Continuous Monitoring Plan (with all appendices) Appendix A: Software Asset Inventory Report Appendix B: Hardening Guides/Configuration baselines for each platform/software product used within the information system Appendix C: Database Configuration Scan results Appendix D: System Asset Inventory (using the inventory template) Appendix E: Hardware Asset Inventory Report generated by automated tool Appendix F: OS Vulnerability scan results Appendix G: Web Vulnerability scan results Appendix H: Code scan results Appendix I: FISMA Assessment Results Appendix J: Plan of Action and Milestones (POA&M) Appendix K: Configuration Management Plan Appendix L: IT Contingency Plan and Contingency Plan Test Results Appendix M: Incident Response Plan and Incident Response Plan Test Results Appendix N: System Security Plan Appendix O: Privacy Impact Assessment (PIA) Appendix P: Penetration Test Results Appendix Q: Self-Attestation Memo
Latest Security Assessment Report
Ongoing Security Authorization Letter

Appendix C: GSA Defined Cloud Controls

The following table contains GSA's assignment parameters for selected NIST 800-53 controls in FedRAMP's Low and Moderate baselines. These parameter settings must be used by CSPs working with GSA pursuing an authorization under the FedRAMP program. CSPs must also address the other controls in FedRAMP's baselines using FedRAMP's assignment parameters.

Table C-1. GSA Parameters for Select FedRAMP Controls

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
Account Management				
AC-2(5)	Account Management	FIPS 199 Moderate and High impact systems shall automatically terminate: (a) A remote access connection after thirty (30) minutes of inactivity; (b) An Internet accessible application session after thirty (30) minutes of inactivity; or (c) A non-interactive user session after thirty (30) – sixty (60) minutes of inactivity. Static web sites and long running operations (e.g., batch jobs) are not subject to this time limit.	Not Applicable	AC-2(5)
AC-2(7)	Account Management	(c) explicit removal actions	Not Applicable	AC-2(7)
AC-2(9)	Account Management	NA - No shared/group accounts in CMP.	Not Applicable	AC-2(9)
AC-2(12)	Account Management	(a) atypical times of day and originating IP address for a known privileged account user that are inconsistent with normal usage patterns (b) the ISSO and the GSA OCISO	Not Applicable	AC-2(12)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
AC-4(21)	Information Flow Enforcement	(1) firewalls; host based firewalls; load balancers; subnets; DMZs; VPC, AWS Security Groups, IAM rules (for systems in AWS); to be approved by the GSA OCISO. (2) segregation of private/system-level information systems and data from public/external information systems and data AND achievement of secure logical system specific ATO boundaries IF providing hosted platform services where hosted application require separate authorizations to operate	Not Applicable	AC-4(21)
Security Assessment and Authorization				
CA-2(2)	Security Assessments	(1) annual (2) announced (3) penetration testing and optionally other activities, such as vulnerability scanning, in-depth monitoring, malicious user testing, insider threat assessment, performance/load testing; (4) continuous monitoring	Not Applicable	CA-2(2)
CA-2(3)	Security Assessments	(1) a FedRAMP authorized information system (2) any FedRAMP accredited 3PAO (3) the conditions of a P-ATO in the FedRAMP Secure Repository	Not Applicable	CA-2(3)
CA-3(3)	System Interconnections	(1) system ATO boundary (i.e., CMP); (2) boundary protections which meet Trusted Internet Connection (TIC) requirements	Not Applicable	CA-3(3)
CA-3(5)		(1) deny-all, permit-by-exception (2) CMP components	Not Applicable	CA-3(5)
Configuration Management				
CM-5(3)	Access Restrictions for Change	software and firmware components	Not Applicable	CM-5(3)
CM-6(1)	Configuration Settings	operating systems	Not Applicable	CM-6(1)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
CM-7(5)	Least Functionality	(a) all authorized software as defined in the Software Inventory in Section 9.2 of the SSP and under CM-8, Information System Component Inventory (c) annually	Not Applicable	CM-7(5)
CM-10(1)	Software Usage Restrictions	follow GSAIT Open Source Policy Framework	Not Applicable	CM-10(1)
Contingency Planning				
CP-9(3)	Information System Backup	the information systems inventory and critical software components such as applications and operating systems software	Not Applicable	CP-9(3)
Identification and Authentication				
IA-5(3)	Authenticator Management	(1) multifactor authenticator tokens and passwords (2) in person (3) a GSA approved registration authority (4) a GSA authorized official	Not Applicable	IA-5(3)
IA-5(4)	Authenticator Management	password complexity requirements defined in IA5 (1) **NOTE:** The idea here is the password complexity is automatically enforced at creation; if such a capability does not exist than it can be addressed through assessment including scanning, pen testing, and security controls assessment.	Not Applicable	IA-5(4)
IA-5(11)	Authenticator Management	HSPD-12 SmartCard requirements	IA-5(11)	IA-5(11)
Incident Response				
IR-9	Information Spillage Response	(b) the GSA Incident Response Team in the OCISO Organization following the reporting procedures identified in GSA IT Security Procedural Guide 01-02, Incident Response (f) incident post mortem and updates to process, procedures, training to minimize the risk of recurrence	Not Applicable	IR-9

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
IR-9(1)	Information Spillage Response	the GSA Incident Response Team in the OCISO Organization	Not Applicable	IR-9(1)
IR-9(2)	Information Spillage Response	annually as part of IR training (see IR-2)	Not Applicable	IR-9(2)
IR-9(3)	Information Spillage Response	reversion to last known backup, fail-over to alternate, new virtual instance, or alternate method to be reviewed and accepted by the OCISO	Not Applicable	IR-9(3)
IR-9(4)	Information Spillage Response	notification and awareness procedures detailing responsibilities and restrictions **NOTE:** Procedures shall reflect relevant federal laws, directives, agency policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.	Not Applicable	IR-9(4)
Physical and Environmental Protection				
PE-13(2)	Fire Protection	NA for CMP; control is AWS responsibility	Not Applicable	PE-13(2)
System and Services Acquisition				
SA-9(4)	External Information System Services	(1) FedRAMP or Federally authorized to operate third-party service providers AND/OR documented MOUs with OCISO approval (2) all external systems where Federal information is processed or stored.	Not Applicable	SA-9(4)
SA-9(5)	External Information System Services	(1) information processing, information data, AND information services (2) FedRAMP-approved data centers (3) the FIPS 199 security categorization requirements for the CMP.	Not Applicable	SA-9(5)
System and Communications Protection Policy and Procedures				
SC-6	Resource Priority	(1) additional resources (2) priority (3) of service provisions	Not Applicable	SC-6
SC-7(8)	Boundary Protection	(1) outbound customer traffic (2) the Internet	Not Applicable	SC-7(8)

CNTL No.	Control Name	GSA Organization-Defined Settings (for controls where 800-53 requires an organizational defined setting/frequency)	Low	Moderate
SC-7(12)	Boundary Protection	host based firewall or Intrusion prevention system (IPS); servers	Not Applicable	SC-7(12)
SC-12(3)	Cryptographic Key Establishment and Management	approved PKI Class 3 certificates or prepositioned keying material	Not Applicable	SC-12(3)
System and Information Integrity				
SI-2(3)	Flaw Remediation	(b) 30 days as the benchmark for Critical/Very High/High-risk vulnerabilities and 90 days as the benchmark for Moderate-risk vulnerabilities.	Not Applicable	SI-2(3)
SI-6	Security Functionality Verification	(a) high security functions (b) upon system startup and/or restart; at least every 90 days (c) system administrator (d) halts the information system, or triggers audit alerts when unauthorized modifications to critical security files occur and	Not Applicable	SI-6

Appendix D: Scanning Frequency By A&A Process

Scanning/testing frequency by component type and A&A process are listed in the 06-30 Scanning Parameter Spreadsheet.